CISA RANSOMWARE CAMPAIGN: REDUCE THE RISK OF RANSOMWARE

NIST NCCOE MANUFACTURING COMMUNITY OF INTEREST WEBINAR
FEBRUARY 25, 2021

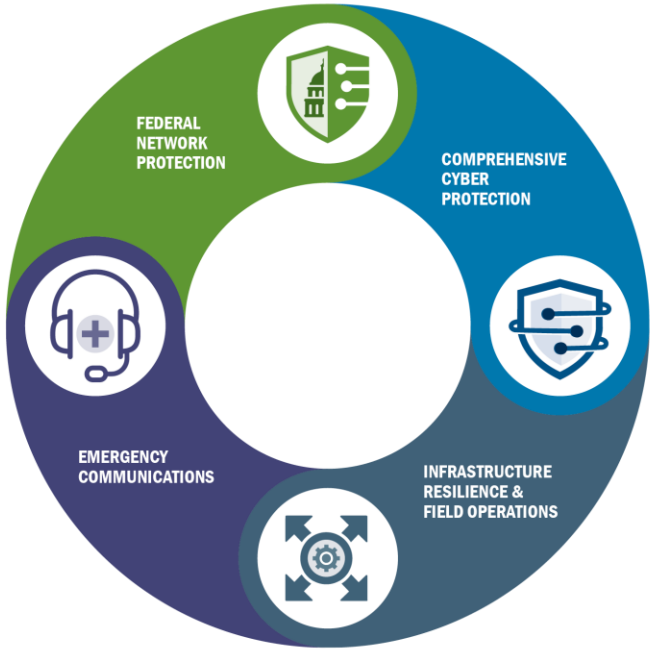
Amy Nicewick
Section Chief
CISA Cybersecurity Division

Cybersecurity and Infrastructure Security Agency (CISA)

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

We are the Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

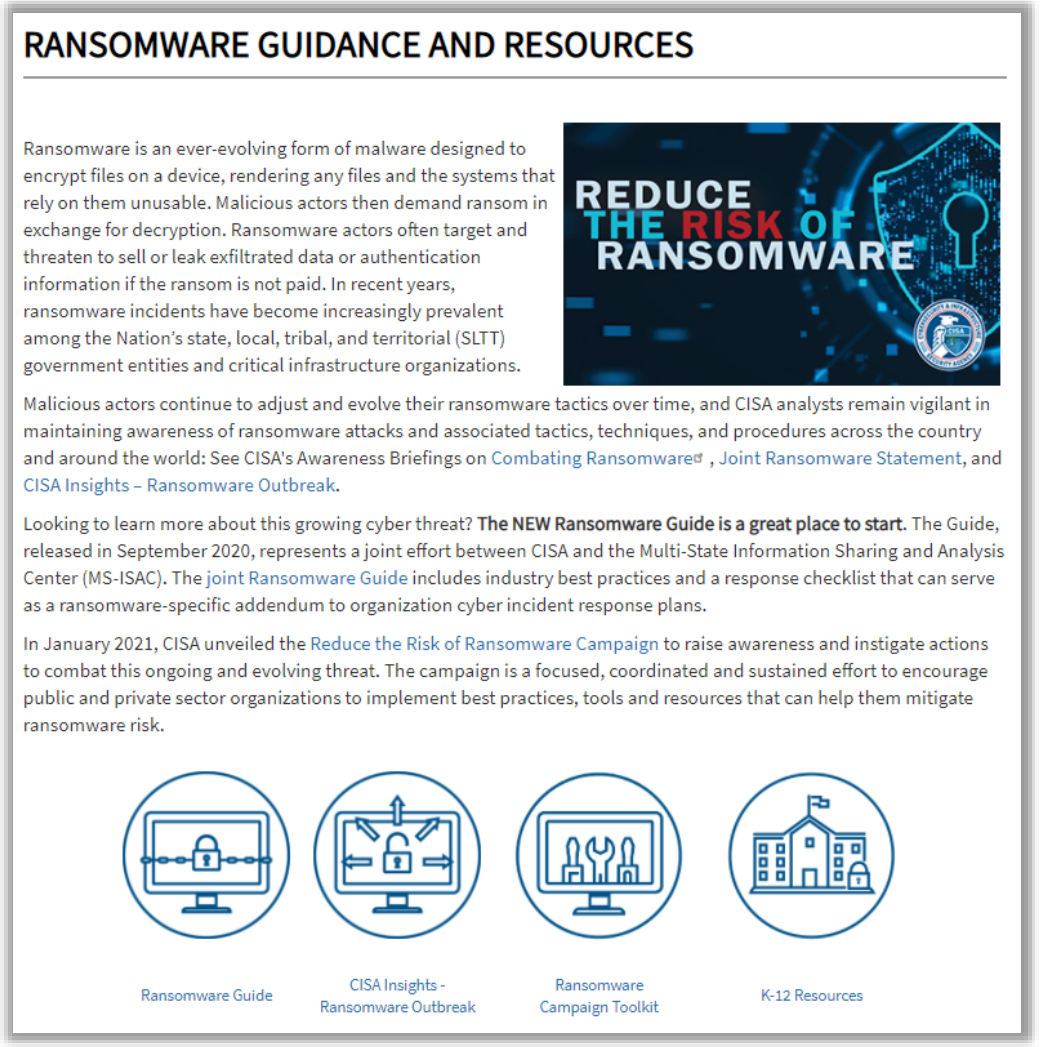
Ransomware Campaign Overview

Ransomware Key Messages

CISA Ransomware Resources

CISA.gov/ransomware

- **Ransomware Guide**
- **CISA INSIGHTS: Ransomware Outbreak**
- **NEW! Toolkit, fact sheet, and images**
- **Alerts and Statements**
  - US-CERT activity alerts on ransomware threats
  - Joint statements on ransomware with our partners
- **Guides and Services**
  - Cyber Hygiene Services
  - TTX Exercises
- **Factsheets and Infographics**
  - Protect Your Center From Ransomware poster
  - Ransomware: What It Is and What To Do About It
- **Training and Webinars**
  - Trends and Predictions in Ransomware (Cyber Summit 2020)
  - CDM Training
  - Incident Response Training Series
  - Combating Ransomware Webinar



RANSOMWARE GUIDANCE AND RESOURCES

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Malicious actors continue to adjust and evolve their ransomware tactics over time, and CISA analysts remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world: See CISA's Awareness Briefings on Combating Ransomware , Joint Ransomware Statement, and CISA Insights – Ransomware Outbreak.

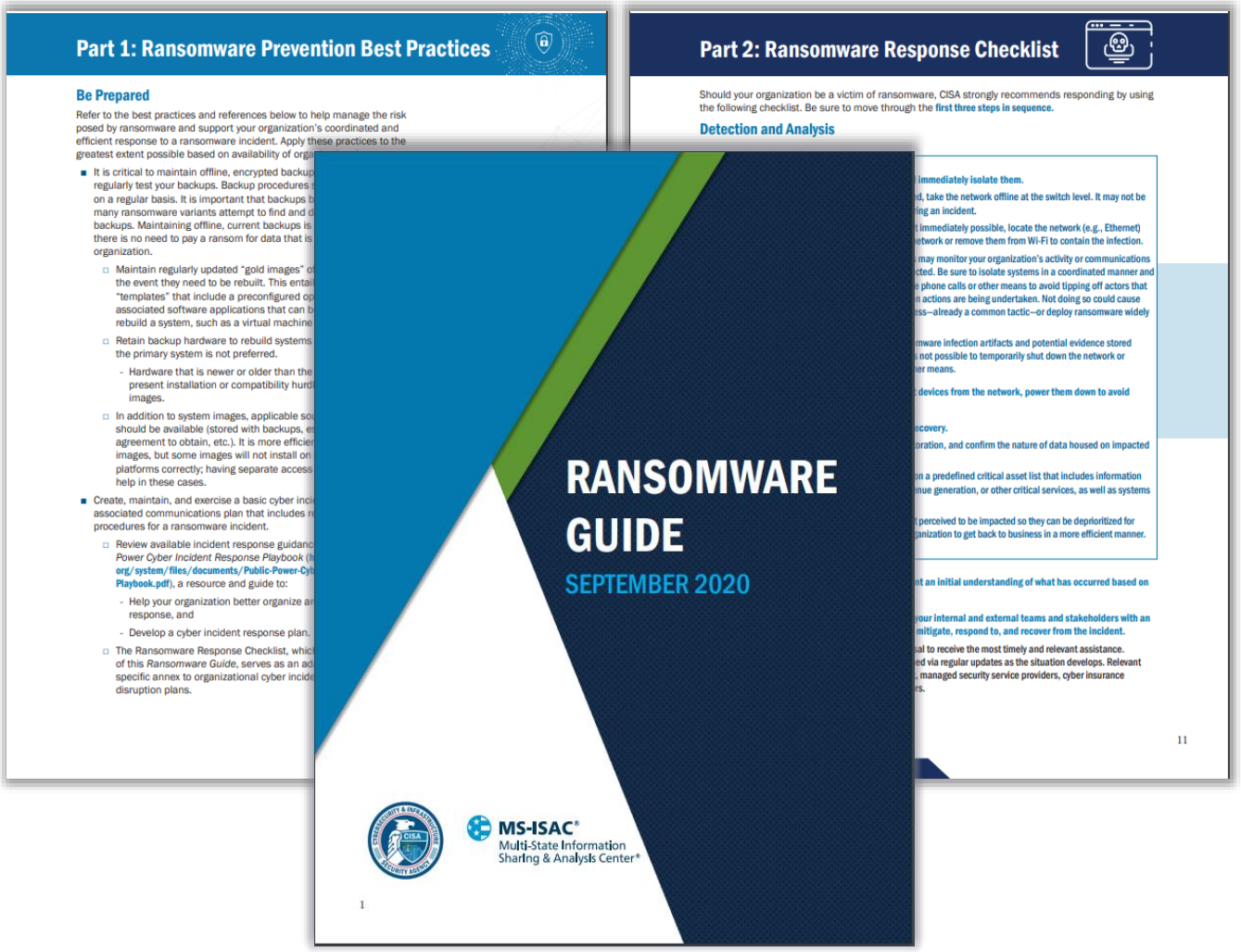
Looking to learn more about this growing cyber threat? **The NEW Ransomware Guide is a great place to start.** The Guide, released in September 2020, represents a joint effort between CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The joint Ransomware Guide includes industry best practices and a response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans.

In January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and instigate actions to combat this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that can help them mitigate ransomware risk.

Ransomware Guide

Joint CISA and MS-ISAC Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks.



Ransomware Response Checklist

Detection and Analysis

- Determine systems impacted, immediately isolate + triage impacted systems for restoration/recovery
- Engage internal/external stakeholders - help to mitigate, respond to, and recover from incident

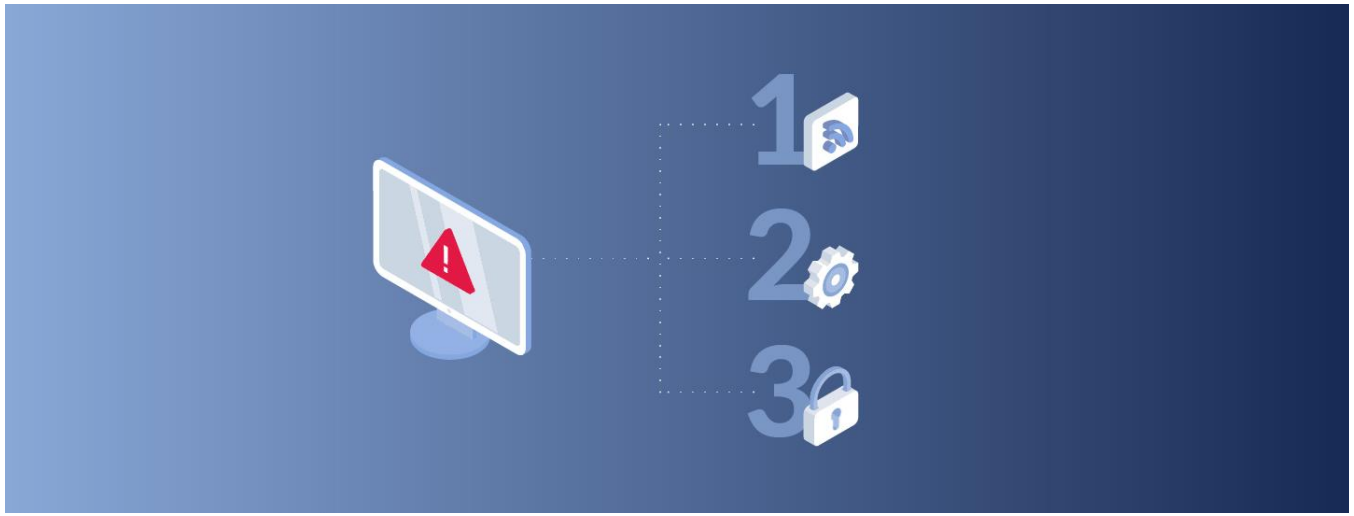
Containment and Eradication

- Investigation: take a system image and memory capture of a sample of affected devices
- Research trusted guidance for ransomware variant + conduct examination of IDS/IPS and logs
- Conduct extended analysis to identify persistence mechanisms
- Rebuild systems based on a prioritization of critical services
- IT security authority declares the incident over

Ransomware Response Checklist

Recovery and Post-Incident Activity

- Reconnect systems, restore data from offline, encrypted backups based on critical services prioritization
- Document lessons learned from the incident
- Consider sharing lessons learned and relevant indicators of compromise (IOCs) with CISA and sector ISAC/ISAO



Ransomware Response Checklist

Who to Contact?

Federal Asset Response: CISA

CISA can assist with analysis at no cost to support your organization in understanding the root cause of the incident (CISA Advanced Malware Analysis Center and Remote Assistance request).

Federal Threat Response: FBI, USSS

For No-Cost Resources Contact:

Federal and SLTT Organizations: CyberLiaison_SLTT@cisa.dhs.gov

Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Campaign Resources: cisa.gov/Ransomware

Vulnerability Scanning

Scanning of internet-accessible systems for known vulnerabilities or potential points of exploit on a continuous basis. As potential vulnerabilities are identified, CISA notifies the organization via proactive notifications and weekly reports so that risk mitigation efforts may be implemented to avoid exploitation.

How to Sign Up

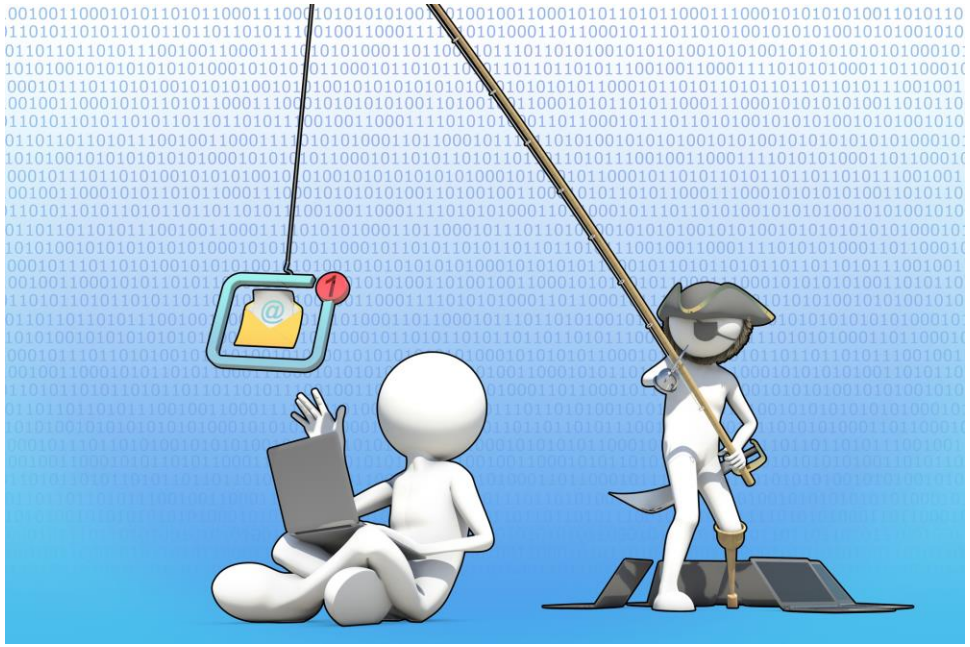
Email CISA at vulnerability_info@cisa.dhs.gov with the subject line “Request Vulnerability Scanning Services” to get started!

Phishing Campaign Assessment

Known as a PCA, this service evaluates an organization's susceptibility and reaction to phishing emails of varying complexity. Deliverable: Report that highlights organizational click rates for varying types of phishing emails and summarizes metrics related to proclivity of the organization to fall victim to phishing attacks and attempts.

How to Sign Up

Email CISA at vulnerability_info@cisa.dhs.gov with the subject line "Request Phishing Campaign Assessment Service" to get started!



Assessments

Cyber Resilience Review

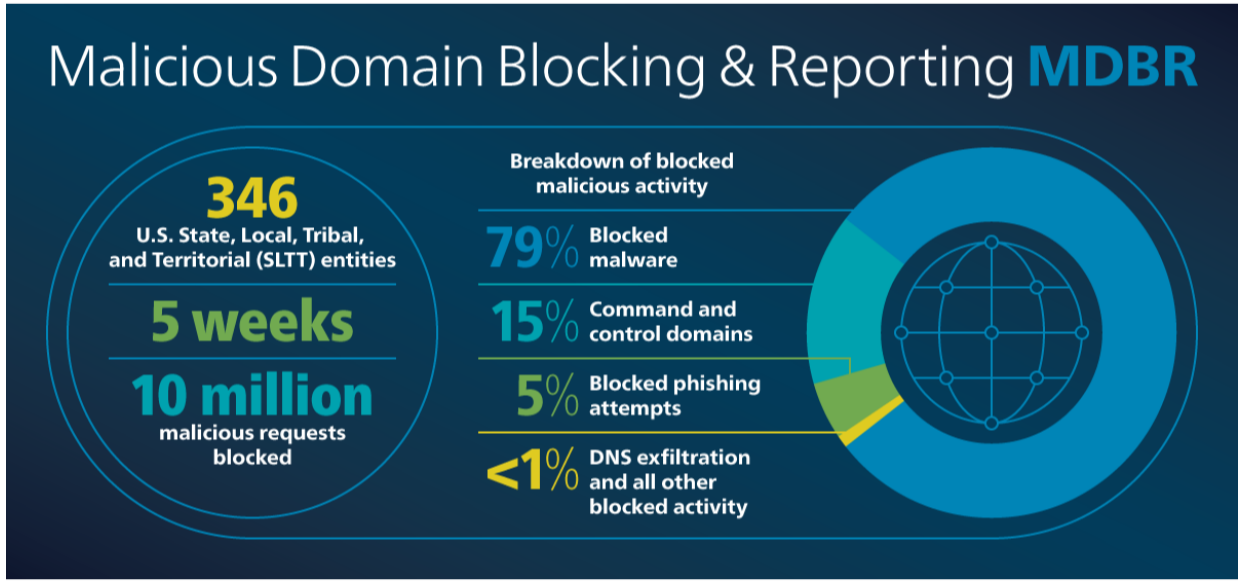
- An interview-based assessment that **evaluates an organization's operational resilience and cybersecurity practices** to provide an organization with greater awareness of its network posture. Evaluates the maturity of an organization in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains.

Cyber Infrastructure Survey

- This is used to **assess an organization's critical services** against cybersecurity controls grouped into five domains. **Organizations receive access to a user-friendly dashboard** to review the results and findings of the survey.

Malicious Domain Blocking and Reporting

- MDBR is funded by CISA, our MS-ISAC and EI-ISAC partners provide the MDBR service at no-cost to members
- Fully managed proactive security service (protective DNS resolver) that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known ransomware, as well as other malware, phishing, and cyber threats.
- To sign up for MDBR, visit: https://www.cisecurity.org/ms-isac/services/mdbr/



Nationwide Cybersecurity Review

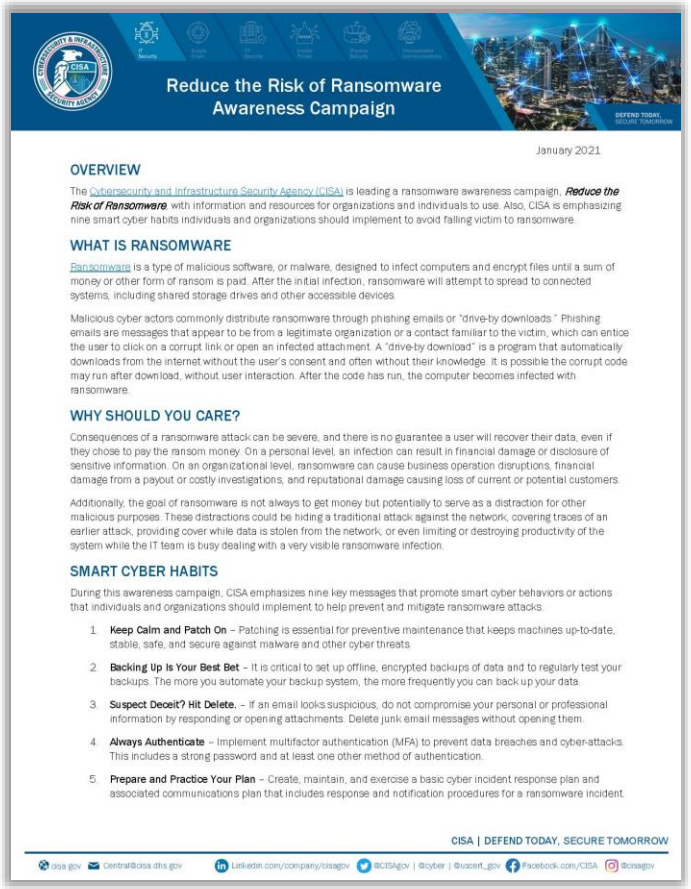
Nationwide Cybersecurity Review (NCSR)

- Conducted by MS-ISAC on CISA's behalf, this review is based on NIST Cybersecurity Framework.
- Anonymous, annual self-assessment to measure gaps/capabilities of SLTT gov't cybersecurity programs.
- Evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents.
- Requirement for Homeland Security Grant Program recipients.

https://www.cisecurity.org/ms-isac/services/ncsr

Ransomware Campaign Toolkit

We recently released a new Ransomware Campaign Toolkit on our ransomware webpage!



Reduce the Risk of Ransomware Awareness Campaign

January 2021

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) is leading a ransomware awareness campaign, ***Reduce the Risk of Ransomware***, with information and resources for organizations and individuals to use. Also, CISA is emphasizing nine smart cyber habits individuals and organizations should implement to avoid falling victim to ransomware.

WHAT IS RANSOMWARE

Ransomware is a type of malicious software, or malware, designed to infect computers and encrypt files until a sum of money or other form of ransom is paid. After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible devices.

Malicious cyber actors commonly distribute ransomware through phishing emails or "drive-by downloads." Phishing emails are messages that appear to be from a legitimate organization or a contact familiar to the victim, which can entice the user to click on a corrupt link or open an infected attachment. A "drive-by download" is a program that automatically downloads from the internet without the user's consent and often without their knowledge. It is possible the corrupt code may run after download, without user interaction. After the code has run, the computer becomes infected with ransomware.

WHY SHOULD YOU CARE?

Consequences of a ransomware attack can be severe, and there is no guarantee a user will recover their data, even if they chose to pay the ransom money. On a personal level, an infection can result in financial damage or disclosure of sensitive information. On an organizational level, ransomware can cause business operation disruptions, financial damage from a payout or costly investigations, and reputational damage causing loss of current or potential customers.

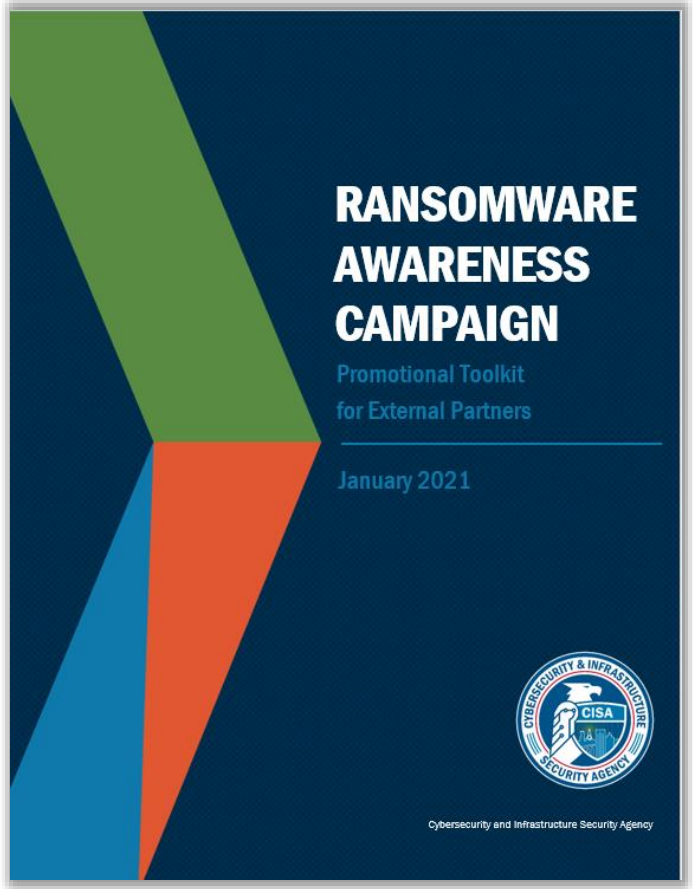
Additionally, the goal of ransomware is not always to get money but potentially to serve as a distraction for other malicious purposes. These distractions could be hiding a traditional attack against the network, covering traces of an earlier attack, providing cover while data is stolen from the network, or even limiting or destroying productivity of the system while the IT team is busy dealing with a very visible ransomware infection.

SMART CYBER HABITS

During this awareness campaign, CISA emphasizes nine key messages that promote smart cyber behaviors or actions that individuals and organizations should implement to help prevent and mitigate ransomware attacks.

1. **Keep Calm and Patch On** – Patching is essential for preventive maintenance that keeps machines up-to-date, stable, safe, and secure against malware and other cyber threats.
2. **Backing Up Is Your Best Bet** – it is critical to set up offline, encrypted backups of data and to regularly test your backups. The more you automate your backup system, the more frequently you can back up your data.
3. **Suspect Deceit? Hit Delete.** – If an email looks suspicious, do not compromise your personal or professional information by responding or opening attachments. Delete junk email messages without opening them.
4. **Always Authenticate** – Implement multifactor authentication (MFA) to prevent data breaches and cyber-attacks. This includes a strong password and at least one other method of authentication.
5. **Prepare and Practice Your Plan** – Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

CISA | DEFEND TODAY, SECURE TOMORROW



For more information:
cisa.gov/ransomware

Contact:

Amy.Nicewick@CISA.dhs.gov

(703) 203-0634